## REMARKS

Claims 19-28 have been cancelled. Claims 1, 37, and 38 have been amended to clarify the subject matter regarded as the invention. Claims 1-18 and 29-38 are pending.

### *Claim Rejections – 35 U.S.C. §101*

Claim 1 has been amended in a manner believed to overcome the Examiner's rejection of that Claim under 35 U.S.C. §101. Claims 2-18 depend from Claim1 and their rejection under 35 U.S.C. §101 is therefore also believed to have been overcome.

Claim 38 has been amended in a manner believed to overcome the Examiner's rejection of that Claim under 35 U.S.C. §101.

### *Claim Rejections – 35 U.S.C. §103(a)*

Independent Claims 1, 37, and 38 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Schultz (US 2003/0065926) and Jordan (7,210,040). The rejections are respectfully traversed.

Schultz describes detecting malicious executables by analyzing byte sequences extracted from the binary code of such executables and applying a set of detection rules designed to detect sequences associated with malicious code. (Schultz, [0104]-[0106] and [0109].) Executables for which a definitive determination cannot be made using existing rules are designated as borderline. (Schultz, [0098].) In Schultz, the rule set is updated periodically, based on offline analysis by experts of the borderline executables. (Schulz, [0107] and [0108].) The analysis described by Schultz is performed statically on binary code comprising the executable, prior to the executable being allowed to execute on a system to which it has been sent. Purely static analysis (i.e., not while the executable is executing), with periodic offline refinement of a set of rules used to perform the static analysis, is not the same as "observ[ing] that a process started by the executable has performed or has attempted to perform an action with which a second risk level, being a higher level than the first, is associated," as recited in independent Claims 1, 37, and 38.

Jordan describes a system for detecting computer viruses that includes an emulator. In Jordan, the "[e]xecution of computer executable code in a subject file is **emulated** by **emulator**

31." (5:36-38). Jordan explains that "[w]hile the program file is being **emulated**, monitor component 32 monitors the code execution... [and] detector component 33 detects an attempt by the **emulated** code to access one or more of the restricted computer system resources." (5:38-47). Emulating the execution of executable code in a file (which requires the presence of an emulator) is not the same as "observ[ing] that a process **started by the executable**" has either "performed or has attempted to perform an action with which a second risk level, being a higher level than the first."

As neither Schultz, nor Jordan, whether considered individually or in combination, disclose all of the limitations of independent Claims 1, 37, and 38, Claims 1, 37, and 38 are therefore believed to be allowable.

Claims 2-18 and 29-36 depend from Claim 1 and are believed to be allowable for the same reasons described above.

The foregoing amendments are not to be taken as an admission of unpatentability of any of the claims prior to the amendments.

Reconsideration of the application and allowance of all claims are respectfully requested based on the preceding remarks. If at any time the Examiner believes that an interview would be helpful, please contact the undersigned.

Respectfully submitted,

Dated: 5/14/09

Robyn Wagner
Registration No. 50,575
V 408-973-2596
F 408-973-2595

VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014